

# Equivalence of Quasi-cyclic Codes over Finite Fields

Kenza Guenda and T. Aaron Gulliver \*

## Abstract

This paper considers the equivalence problem for quasi-cyclic codes over finite fields. The results obtained are used to construct isodual quasi-cyclic codes.

## 1 Introduction

The equivalence problem for codes has numerous practical applications such as code-based cryptography [10, 11, 13]. As a consequence, many researchers have considered this problem [1, 3, 12, 13], but to date there has been little progress in obtaining a solution. Brand [2] characterized the set of permutations by which two combinatorial cyclic objects on  $p^r$  elements are equivalent. Using these results, Huffman et al. [3] explicitly gave this set in the case  $n = p^2$  and provided algorithms to determine the equivalence between cyclic objects and extended cyclic objects. In [3], a negative answer was given to the generalization of their results to the case  $n = p^r$ ,  $r > 2$ . Babai et al. [1] gave an exponential time algorithm for determining the equivalence of codes. Sendrier [12] proposed the support splitting algorithm to solve the problem of code equivalence in the binary case. Unfortunately, in [13] it was shown that extending this algorithm to  $q \geq 5$  has an exponential growth in complexity.

In this paper, the equivalence problem is studied for quasi-cyclic codes over finite fields. It is proven that two quasi-cyclic codes are equivalent if and only if their constituent codes are equivalent. This is an important result which allows conditions to be given on the existence of isodual quasi-cyclic codes. These conditions are used to obtain constructions of isodual quasi-cyclic codes.

The remainder of this paper is organized as follows. In Section 2, some preliminary definitions and results are given. The main result is presented in Section 3. It is proven that two quasi-cyclic codes are equivalent if and only if their constituent codes are equivalent. In Section 4, we introduce multiplier equivalent cyclic codes. Further, we examine the

---

\*K. Guenda is with the Faculty of Mathematics USTHB, University of Science and Technology of Algiers, Algeria. T. Aaron Gulliver is with the Department of Electrical and Computer Engineering, University of Victoria, PO Box 1700, STN CSC, Victoria, BC, Canada V8W 2Y2. email: agullive@ece.uvic.ca. This work is an extension version of a part of Ph.D thesis of K. Guenda

equivalence of quasi-cyclic codes with cyclic constituent codes. Section 5 then considers conditions on the existence of isodual quasi-cyclic codes.

## 2 Preliminaries

Let  $C$  be a linear code of length  $n$  over a finite field  $\mathbb{F}_q$ , and  $\sigma$  a permutation of the symmetric group  $S_n$  acting on  $\{0, 1, \dots, n-1\}$ . We associate with this code a linear code  $\sigma(C)$  defined by

$$\sigma(C) = \{(x_{\sigma^{-1}(0)}, \dots, x_{\sigma^{-1}(n-1)}); (x_0, \dots, x_{n-1}) \in C\}.$$

We say that the codes  $C$  and  $C'$  are equivalent if there exists a permutation  $\sigma \in S_n$  such that  $C' = \sigma(C)$ . The automorphism group of  $C$  is the subgroup of  $S_n$  given by

$$\text{Aut}(C) = \{\sigma \in S_n; \sigma(C) = C\}.$$

A linear code  $C$  of length  $n$  over  $\mathbb{F}_q$  is called quasi-cyclic of index  $l$  or an  $l$ -quasi-cyclic code if its automorphism group contains the permutation  $T^l$  given by

$$\begin{aligned} T^l : \mathbb{Z}_n &\longrightarrow \mathbb{Z}_n \\ i &\longmapsto i + l \pmod{n}. \end{aligned} \tag{1}$$

This definition is equivalent to saying that for all  $c \in C$  we have  $T^l(c) \in C$  with  $T : i \mapsto i+1$  being the circular shift. The index  $l$  of  $C$  is the smallest integer satisfying this property. It can easily be proven that  $l$  is a divisor of  $n$ . If  $l = 1$  the code  $C$  is called a cyclic code. The automorphism group of  $C$  then contains the cyclic shift  $T$ . A cyclic code over  $\mathbb{F}_q$  of length  $n$  is an ideal of the ring  $\mathbb{F}_q[x]/(x^n - 1)$ . Hence it is generated by a polynomial  $f(x)|(x^n - 1)$ . For a primitive element  $\alpha$  of  $\mathbb{F}_q$ , the defining set  $T$  of a cyclic code is a subset of  $\mathbb{Z}_n$ ;  $T = \{i \leq n, f(\alpha^i) = 0\}$ . There is a one-to-one correspondence between the irreducible factors of  $f(x)$  and subsets of  $T$ . These subsets are called the cyclotomic classes.

Let  $a$  and  $n$  be positive integers such that  $\gcd(a, n) = 1$ . The permutation  $\mu_a$  defined on  $\mathbb{Z}_n = \{0, 1, \dots, n\}$  by

$$\begin{aligned} \mu_a : \mathbb{Z}_n &\longrightarrow \mathbb{Z}_n \\ i &\longmapsto \mu_a(i) = ia, \end{aligned} \tag{2}$$

is called a multiplier. Multipliers play an essential role in code equivalence [?]. We attach the standard inner product to  $\mathbb{F}_q^n$

$$[v, w] = \sum v_i w_i.$$

The Euclidean dual code  $C^\perp$  of  $C$  is defined as

$$C^\perp = \{v \in \mathbb{F}_q^n; [v, w] = 0 \text{ for all } w \in C\}. \tag{3}$$

If  $C \subseteq C^\perp$ , the code is said to be self-orthogonal, and if  $C = C^\perp$  the code is self-dual. We call an isodual code a linear code which is equivalent to its dual.

Let  $f(x) = a_0 + a_1x + \dots + a_rx^r$  be a polynomial of degree  $r$  with  $f(0) = a_0 \neq 0$ . Then the monic reciprocal polynomial of  $f(x)$  is

$$f^*(x) = f(0)^{-1}x^r f(x^{-1}) = a_0^{-1}(a_r + a_{r-1}x + \dots + a_0x^r).$$

If a polynomial is equal to its reciprocal then it is called a self-reciprocal polynomial.

### 3 Equivalent Quasi-cyclic Codes

In this section, we characterize the equivalence problem for quasi-cyclic codes.

Let  $\mathbb{F}_q$  be the finite field of cardinality  $q$  and  $m$  be a positive integer such that  $\gcd(m, q) = 1$ . Further, let  $\mathbb{F}_q[Y]$  denote the ring of polynomials in the indeterminate  $Y$  over  $\mathbb{F}_q$ . Define the ring  $R = \mathbb{F}_q[Y]/(Y^m - 1)$ , and for a positive integer  $l$  define the following map

$$\begin{aligned} \Phi : \mathbb{F}_q^{lm} &\longrightarrow R^l \\ c = (c_{0,0}, c_{0,1}, \dots, c_{0,l-1}, \dots, c_{r-1,0}, \dots, c_{r-1,l-1}) &\longmapsto \Phi(c) = (c_0(Y), c_1(Y), \dots, c_{l-1}(Y)), \end{aligned} \quad (4)$$

where  $c_j(Y) = \sum_{i=0}^{m-1} c_{i,j} Y^i \in \mathbb{F}_q$ . It was shown in [8] that the map  $\Phi$  induce a one-to-one correspondence between quasi-cyclic codes over  $\mathbb{F}_q$  of index  $l$  and length  $lm$  and linear codes over  $R$  of length  $l$ .

Note that in (4) each coordinate  $c_{i,j}$  in  $c = (c_{0,0}, \dots, c_{0,l-1}, \dots, c_{m-1,0}, \dots, c_{m-1,l-1})$  can be written as  $c_{j+il}$ ,  $0 \leq j \leq l-1$ ,  $1 \leq i \leq m-1$ . Now  $c_j(Y) = \sum_{i=0}^{m-1} c_{i,j} Y^i \in R$  can be expressed its vectorial form as  $c_j(Y) = (c_{0,j}, c_{1,j}, \dots, c_{m-1,j})$ . Then the image of the codeword  $(c_{j+il})_{0 \leq j \leq l-1; 1 \leq i \leq m-1}$  by the map  $\Phi$  is the codeword  $(c_{i+jm})_{0 \leq j \leq l-1; 1 \leq i \leq m-1}$ . This suggests the following result.

**Proposition 3.1** *Let  $\mathcal{C}$  and  $\mathcal{C}'$  be quasi-cyclic codes of length  $lm$  and index  $l$  over  $\mathbb{F}_q$ . Then  $\mathcal{C}$  and  $\mathcal{C}'$  are equivalent if and only if the codes  $C = \Phi(\mathcal{C})$  and  $C' = \Phi(\mathcal{C}')$  are equivalent.*

**Proof.** Assume that  $\mathcal{C} = \{(c_{j+il})_{0 \leq j \leq l-1; 1 \leq i \leq m-1}\}$  and  $\mathcal{C}' = \{(c'_{j+il})_{0 \leq j \leq l-1; 1 \leq i \leq m-1}\}$  are equivalent by a permutation  $\sigma \in S_n$ . Hence if  $\sigma$  is such that  $\sigma(j+il) = j' + i'l$ , then we have  $\sigma((c_{j+il})_{0 \leq j \leq l-1; 1 \leq i \leq m-1}) = (c'_{j+il})_{0 \leq j \leq l-1; 1 \leq i \leq m-1} = (c_{j'+i'l})_{0 \leq j' \leq l-1; 1 \leq i' \leq m-1}$ . Hence

$$\Phi(\sigma((c_{j+il})_{0 \leq j \leq l-1; 1 \leq i \leq m-1})) = \Phi((c_{j'+i'l})_{0 \leq j' \leq l-1; 1 \leq i' \leq m-1}) = (c_{i'+j'm})_{0 \leq j' \leq l-1; 1 \leq i' \leq m-1},$$

and we have an associated permutation  $\tau$  given by  $\tau(i' + j'm) = i + jm$ . Since  $\sigma$  is in  $S_n$ ,  $\tau$  is also in  $S_n$ . Furthermore,  $\tau$  is such that  $\tau(\Phi(\sigma(\mathcal{C}))) = \Phi(\mathcal{C})$ . This proves the first implication.

Now assume that  $C = \{(c_{i+jm})_{0 \leq j \leq l-1; 0 \leq i \leq m-1}\}$  and  $C' = \{(c'_{i+jm})_{0 \leq j \leq l-1; 0 \leq i \leq m-1}\}$  are images by the map  $\Phi$  of two quasi-cyclic codes  $\mathcal{C}$  and  $\mathcal{C}'$ , respectively, and there exists a permutation  $\sigma$  such that  $\sigma(C) = \sigma(\{(c_{i+jm})_{0 \leq j \leq l-1; 0 \leq i \leq m-1}\}) = C' = \{(c'_{i+jm})_{0 \leq j \leq l-1; 0 \leq i \leq m-1}\} = \{(c'_{i'+j'm})_{0 \leq j' \leq l-1; 0 \leq i' \leq m-1}\}$ . Hence  $\mathcal{C} = \{(c_{j+il})_{0 \leq j \leq l-1; 0 \leq i \leq m-1}\}$  and  $\mathcal{C}' = \{(c_{j'+i'l})_{0 \leq j' \leq l-1; 0 \leq i' \leq m-1}\}$ . Then by defining the permutation  $\tau$  such that  $\tau(j' + i'l) = j + il$  we obtain that  $\tau(\mathcal{C}') = \mathcal{C}$ .  $\square$

Now we consider the factorization of  $Y^m - 1$  over  $\mathbb{F}_q$ . Since it is assumed that  $\gcd(m, q) = 1$ ,  $Y^m - 1$  has a unique decomposition into irreducible factors over  $\mathbb{F}_q$

$$Y^m - 1 = \delta g_1 \dots g_s h_1 h_1^* \dots h_t h_t^*, \quad (5)$$

where  $\delta$  is a unit in  $\mathbb{F}_q$ ,  $h_i^*$  is the reciprocal of  $h_i$ , and  $g_i$  is self-reciprocal. The ring  $R$  is a principal ideal ring, so it can be decomposed into a direct sum of local rings. Hence the Chinese Remainder Theorem gives the following decomposition

$$R = \frac{\mathbb{F}_q[Y]}{(Y^m - 1)} = \left( \bigoplus_{i=1}^s \frac{\mathbb{F}_q[Y]}{(g_i)} \right) \oplus \left( \bigoplus_{j=1}^t \left( \frac{\mathbb{F}_q[Y]}{(h_j)} \oplus \frac{\mathbb{F}_q[Y]}{(h_j^*)} \right) \right). \quad (6)$$

Let  $\frac{\mathbb{F}_q[Y]}{(g_i)} = G_i$ ,  $\frac{\mathbb{F}_q[Y]}{(h_j)} = H'_j$ , and  $\frac{\mathbb{F}_q[Y]}{(h_j^*)} = H''_j$ . Since the polynomials in the decomposition (5) are irreducible, the local rings are in fact field extensions of  $\mathbb{F}_q$ . Then as a consequence of the decomposition (6), we obtain that every  $R$ -linear code of length  $l$  can be decomposed as  $C = (\bigoplus_{i=1}^s C_i) \oplus (\bigoplus_{j=1}^t (C'_j \oplus C''_j))$ , where  $C_i$  is a linear code over  $G_i$ ,  $C'_j$  is a linear code over  $H'_j$ , and  $C''_j$  is a linear code over  $H''_j$ . The codes  $C_i$ ,  $C_j$  and  $C''_j$  are called the *components* of the quasi-cyclic code  $\mathcal{C}$ .

Assume that  $g_i$  is one of the self-reciprocal polynomials in (5). We now study the action of the following map over the local component ring  $\mathbb{F}_q[Y]/\langle g_i \rangle = G_j$  of  $R$

$$\begin{aligned} - : \mathbb{F}_q[Y]/\langle g_i \rangle &\longrightarrow \mathbb{F}_q[Y]/\langle g_i \rangle \\ c(Y) &\mapsto c(Y^{-1}). \end{aligned} \quad (7)$$

The map  $-$  is a ring automorphism. For  $g_i$  of degree 1 this map is the identity, and if  $\deg(g_i) = K_i \neq 1$ , since  $g_i$  and  $g_i^*$  are associated,  $K_i$  must be even. Since  $g_i$  is irreducible and square free, it is also separable and local. Further, as  $g_i$  is irreducible of degree  $d_i$ , from [5, Theorem 4.2] the ring  $G_i = \mathbb{F}_q[Y]/\langle g_i \rangle$  is an extension of  $\mathbb{F}_q$ , namely  $\mathbb{F}_{q^{d_i}}$ . Then the map  $r \mapsto \bar{r}$ , is the map  $\nu : r \mapsto r^{q^{K_i/2}}$  and is a power of the Frobenius map. Hence, it is a permutation over  $\mathbb{F}_{q^{d_i}}$  which fixes the elements of  $\mathbb{F}_q$ . This proves the following result.

**Lemma 3.2** *With the previous notation, each code  $C_i$  over  $G_i$  is equivalent to  $\nu(C_i) = \overline{C_i}$ .*

For each  $a = (a_0, \dots, a_{l-1})$ ,  $b = (b_0, \dots, b_{l-1})$  in  $G_i^l$ , we define the Hermitian inner product on  $G_i$  by

$$\langle a, b \rangle^H = \sum_k a b_k^*. \quad (8)$$

This is in fact the usual Hermitian inner product. We now have the following lemma.

**Lemma 3.3** *Let  $C_i$  be a linear code over  $G_i$ . The Hermitian dual of  $C_i$  denoted  $C_i^{\perp H}$  is equivalent to the Euclidean dual of  $C_i$ .*

**Proof.** Define the code  $\overline{C} = \{\overline{r}; r \in C\}$ . It is easy to see that  $C_i^{\perp H} = \overline{(C_i)}^\perp = \nu(C_i)^\perp$ . Hence from Lemma 3.2 we have that  $\nu(C_i)^\perp = (\nu(C_i^\perp))$ .  $\square$

For  $a, b \in \mathbb{F}_q^{lm}$ , let  $\Phi(a) = (a_0, \dots, a_{l-1})$  and  $\Phi(b) = (b_0, \dots, b_{l-1})$ , where

$$a_i = (a_{i,1}, \dots, a_{i,s}, a_{i,1}', a_{i,1}'', \dots, a_{i,t}' a_{i,1}''),$$

and

$$b_i = (b_{i,1}, \dots, b_{i,s}, b_{i,1}', b_{i,1}'', \dots, b_{i,t}' b_{i,1}''),$$

with  $a_{i,j}, b_{i,j} \in G_j$ ,  $a_{i,j}', b_{i,j}' \in H_j'$ , and  $a_{i,j}'', b_{i,j}'' \in H_j''$ .

We define the Hermitian inner product on  $R^l$  by

$$\begin{aligned} \langle \Phi(a), \Phi(b) \rangle &= \left( \sum_i a_{i,1} \overline{b_{i,1}}, \dots, \sum_i a_{i,s} \overline{b_{i,s}}, \right. \\ &\quad \sum_i a_{i,1}' b_{i,1}'', \sum_i a_{i,1}'' b_{i,1}', \dots \\ &\quad \left. \sum_i a_{i,t}' b_{i,t}'', \sum_i a_{i,t}'' b_{i,t}' \right). \end{aligned}$$

Using this inner product, Ling and Solé [8] and Lim [7] gave the Euclidean dual of a quasi-cyclic code.

**Proposition 3.4** *Let  $\mathcal{C}$  be an  $l$ -quasi-cyclic code of length  $lm$  over  $\mathbb{F}_q$  and  $C = \Phi(\mathcal{C}) = (\oplus_{i=1}^s C_i \oplus (\oplus_{j=1}^t (C_j' \oplus C_j'')))$  be its image as defined previously. Then the Euclidean dual of  $\mathcal{C}$  is the  $l$ -quasi-cyclic code  $\mathcal{C}^\perp$  such that  $\Phi(\mathcal{C}^\perp) = (\oplus_{i=1}^s C_i^{\perp H} \oplus (\oplus_{j=1}^t (C_j''^\perp \oplus C_j'^\perp)))$ .*

We require the following lemma concerning the direct sum of codes.

**Lemma 3.5** *Assume that  $C = C_1 \oplus C_2$  and  $C' = C_1' \oplus C_2'$  are codes of length  $2n$  which are the direct sums of codes of length  $n$ . Then there exist a permutation  $\sigma \in S_{2n}$  such that  $\sigma(C) = C'$  if and only if there exist permutations  $\sigma_1$  and  $\sigma_2$  in  $S_n$  such that  $\sigma_1(C_1) = C_1'$  and  $\sigma_2(C_2) = C_2'$ .*

**Proof.** Assume that

$$\sigma(C) = \sigma(C_1 \oplus C_2) = C',$$

and

$$C' = C_1' \oplus C_2' = \{(c_{\sigma(1)}, \dots, c_{\sigma(n)}, c_{\sigma(n+1)}, \dots, c_{\sigma(2n)}), \text{ with } (c_1, \dots, c_n) \in C_1 \text{ and } (c_{n+1}, \dots, c_{2n}) \in C_2\}.$$

This gives that  $\sigma(i) \in \{1, \dots, n\}$  for  $1 \leq i \leq n$ , and  $\sigma(i) \in \{n+1, \dots, 2n\}$  for  $n+1 \leq i \leq 2n$ . Hence we can define the permutations  $\sigma_1$  and  $\sigma_2$  on  $n$  elements by  $\sigma_1(1) = \sigma(1), \dots, \sigma_1(n) = \sigma(n)$ , and  $\sigma_2(1) = \sigma(n+1), \dots, \sigma_2(n) = \sigma(2n)$ . Then  $\sigma(C_1 \oplus C_2) = \sigma_1(C_1) \oplus \sigma_2(C_2) = C'_1 \oplus C'_2$ . Let the mapping  $Pr_1$  be the projection on the first  $n$  coordinates so that  $Pr_1(\sigma_1(C_1) \oplus \sigma_2(C_2)) = \sigma_1(C_1) = Pr_1(C'_1 \oplus C'_2) = C'_1$  and then  $\sigma_1(C_1) = C'_1$ . We also obtain  $\sigma_1(C_2) = C'_2$  by considering the projection  $Pr_2$  on the last  $n$  coordinates. For the converse, assume that there exists permutations  $\sigma_1$  and  $\sigma_2$  such that  $\sigma_1(C_1) = C'_1$  and  $\sigma_2(C_2) = C'_2$ . Hence we obtain the permutation  $\sigma \in S_{2n}$  given by  $\sigma(i) = \sigma_1(i)$ , and  $\sigma(i+n) = \sigma_2(i)$  for  $1 \leq i \leq n$ , so then  $\sigma(C) = C'$ .  $\square$

**Remark 3.6** *Lemma 3.5 is also true for the direct sum of  $k > 2$  codes of the same length.*

**Theorem 3.7** *Let  $\mathcal{C}$  be a quasi-cyclic code of length  $lm$  and index  $l$  over  $\mathbb{F}_q$  such that  $\Phi(\mathcal{C}) = (\oplus_{i=1}^s C_i) \oplus (\oplus_{j=1}^t (C'_j \oplus C''_j))$ . Then  $\mathcal{C}$  is isodual if and only if each of its components  $C_i$  for  $1 \leq i \leq s$  is isodual, and for each  $1 \leq j \leq t$  we have that  $C'_j$  is equivalent to  $C''_j$ .*

**Proof.** Let  $\mathcal{C}$  be an  $l$ -quasi-cyclic code which is isodual. Then there exists a permutation  $\sigma$  such that  $\mathcal{C} = \sigma(\mathcal{C}^\perp)$ . By Proposition 3.1, there exists a permutation  $\tau$  such that  $\Phi(\mathcal{C}) = \tau(\Phi(\mathcal{C}^\perp))$ . From Proposition 3.4 we have that  $\Phi(\mathcal{C}^\perp) = \Phi(\mathcal{C})^{\perp H} = (\oplus_{i=1}^s (C_i^{\perp H}) \oplus (\oplus_{j=1}^t C_j^{\perp H} \oplus C_j^{\perp H}))$ . Hence from Lemma 3.5 there exist permutations  $\tau_i$ ,  $\tau'_j$ , and  $\tau''_j$  such that  $C_i = \tau_i(C_i^{\perp H})$ ,  $C'_j = \tau'_j(C_j^{\perp H})$ , and  $C''_j = \tau''_j(C_j^{\perp H})$ . From Lemma 3.3 we have that  $C_i^{\perp H} = \nu(C_i)^\perp$ , so  $C_i = \tau_i(\nu(C_i)^\perp)$ . Then for  $1 \leq i \leq s$ , the component  $C_i$  is isodual. For the converse, assume that each component of  $\mathcal{C}$  is isodual. Then we have that  $\tau_i(C_i) = C_i^\perp$  for  $1 \leq i \leq s$ ,  $\tau'_j(C'_j) = C_j^\perp$  and  $\tau''_j(C''_j) = (C''_j)^\perp$  for  $1 \leq j \leq t$ . From Lemma 3.3 we have that  $C_i^{\perp H} = \nu(C_i)^\perp$ . Hence  $C_i^{\perp H} = \nu(\tau_i(C_i))$ , so that  $\Phi(\mathcal{C})^\perp = (\oplus \nu(\tau_i(C_i)) \oplus (\oplus \tau'_j(C'_j) \oplus \tau''_j(C''_j)))$ . Then from Lemma 3.5 there exists a permutation  $\theta$  such that  $\Phi(\mathcal{C})^\perp = \theta(\oplus_{i=1}^s C_i) \oplus (\oplus_{j=1}^t (C'_j \oplus C''_j))$ , and by Proposition 3.1  $\mathcal{C}$  is isodual.  $\square$

The following corollary is a direct consequence of Proposition 3.1 and Theorem 3.7. Note that this result was given in [8, Theorem 4.2].

**Corollary 3.8** *An  $l$ -quasi-cyclic code  $\mathcal{C}$  of length  $lm$  over  $R$  is self-dual if and only if*

$$\Phi(\mathcal{C}) = \left( \bigoplus_{i=1}^s C_i \right) \oplus \left( \bigoplus_{j=1}^t (C'_j \oplus (C'_j)^\perp) \right),$$

where for  $1 \leq i \leq s$ ,  $C_i$  is a self-dual code over  $\frac{R[Y]}{(g_i)}$  with respect to the Hermitian inner product, and for  $1 \leq j \leq t$ ,  $C'_j$  is a linear code of length  $l$  over  $H_j$  and  $C_j^{\perp}$  is its dual with respect to the Euclidean inner product.

In [8, Proposition 6.1], conditions were given on the existence of self-dual quasi-cyclic codes of index 2. We generalize these results to give conditions on the existence of self-dual quasi-cyclic codes of index  $l$  even as follows.

**Theorem 3.9** *Let  $m$  be an integer relatively prime to  $q$ . Then self-dual quasi-cyclic codes over  $\mathbb{F}_q$  of length  $lm$ ,  $l$  even, exists if and only if one of the following conditions is satisfied:*

- (i)  $q$  is a power of 2,
- (ii)  $q = p^b$ , where  $p$  is a prime congruent to 1 mod 4, or
- (iii)  $q = p^{2b}$ , where  $p$  is a prime congruent to 3 mod 4.

**Proof.** If a self-dual quasi-cyclic code  $\mathcal{C}$  over of length  $lm$  exists, then Corollary 3.8 shows that there is a self-dual code  $C_1$  of length  $l$  over  $G_1$ . Hence the conditions in the theorem are necessary. Conversely, if any one of the conditions is satisfied, then there exists  $\gamma \in \mathbb{F}_q$  such that  $\gamma^2 + 1 = 0$ . Consequently, every finite extension of  $\mathbb{F}_q$  also contains such an element. Then the code generated by  $(1, \gamma, \dots, 1, \gamma)$  is self-dual over any extension of  $\mathbb{F}_q$  (with respect to both the Euclidean and Hermitian inner products). Hence from Corollary 3.8, a self-dual quasi-cyclic code of length  $lm$  exists over  $\mathbb{F}_q$ .  $\square$

## 4 Multiplier Equivalent Quasi-Cyclic Codes

A natural question that arises is, can a multiplier be a permutation by which two quasi-cyclic codes are equivalent? In the special case of the so-called one-generator quasi-cyclic codes, Ling and Solé defined the multiplier equivalence. However, this definition can be placed in a more general setting than that given in [9], namely there is no need to restrict the definition to one-generator quasi-cyclic codes. From Lemma 3.5 and Proposition 3.4 we have that two quasi-cyclic codes are equivalent if and only if their constituent codes are equivalent. Hence we can give the following definition.

**Definition 4.1** *Two quasi-cyclic codes  $\mathcal{C}$  and  $\mathcal{D}$  are multiplier equivalent if and only if each of their components are multiplier equivalent.*

In the next section, conditions are given on when two quasi-cyclic codes with cyclic components are multiplier equivalent.

### 4.1 Equivalence of Quasi-Cyclic Codes with Cyclic Constituent Codes

In this section, we consider the equivalence of quasi-cyclic codes with cyclic constituent codes, i.e.  $\Phi(\mathcal{C})$  is cyclic or  $\Phi(\mathcal{C})$  is an ideal of  $R[X]/(X^l - 1)$ . We have the following results.

**Proposition 4.2** ([7, Proposition 8]) *Let  $q$  be a prime power and  $\mathbb{F}_q$  the finite field with  $q$  elements. Further, let  $l$  and  $m$  be positive integers with  $m$  coprime to  $q$ , and let  $\mathcal{C}$  be a quasi-cyclic code of length  $lm$  and index  $l$  over  $\mathbb{F}_q$ . Then the following are equivalent*

(i)  $\Phi(\mathcal{C})$  is cyclic, and

(ii) all the constituent codes of  $\mathcal{C}$  are cyclic.

**Theorem 4.3** *Let  $\mathcal{C}$  and  $\mathcal{D}$  be quasi-cyclic codes of length  $pm$  and index  $p$  a prime, both with cyclic constituent codes. Then  $\mathcal{C}$  and  $\mathcal{D}$  are equivalent if and only if they are multiplier equivalent.*

**Proof.** Assume that  $\mathcal{C}$  and  $\mathcal{D}$  are quasi-cyclic codes with cyclic constituent codes. Then from Proposition 4.2 all the constituent codes are cyclic. Furthermore, from Theorem 3.7  $\mathcal{C}$  and  $\mathcal{D}$  are equivalent if and only if their cyclic constituent codes are equivalent. These cyclic codes have length  $p$  a prime. Then from [3, Theorem 1], they are equivalent if and only if they are multiplier equivalent. Hence the result follows.  $\square$

**Remark 4.4** *When  $l = p^\alpha, \alpha > 1$ , there exist other permutations by which two quasi-cyclic codes may be equivalent [?].*

**Theorem 4.5** *Let  $\mathcal{C}$  be a quasi-cyclic code of length  $pm$  and index  $p$  a prime with cyclic constituent codes. Then the number of quasi-cyclic codes equivalent to  $\mathcal{C}$  is  $p^r$ , where  $r$  is equal to the number of irreducible factors of  $Y^m - 1$ .*

**Proof.** Under the previous hypotheses, the components  $C_i, C'_j$  and  $C''_j$  of  $\mathcal{C}$  are cyclic. If  $\mu_a$  is a multiplier, then the quasi-cyclic code with components  $\mu(C_1), C_i, i \neq 1, C'_j$  and  $C''_j$  is equivalent to  $\mathcal{C}$ . This also holds for quasi-cyclic codes with components  $C_1, \mu_a(C_2), C_i, i \neq 2, C'_j$  and  $C''_j$ . It is also true for the quasi-cyclic code with the constituent codes  $\mu_a(C_k), k \in \{1, \leq s\}$  or  $k \in \{1 \leq t\}$  and all others equal to  $C_i, C'_j$  or  $C''_j$ . Since there are  $p - 1$  multipliers and  $r$  components, the number of quasi-cyclic codes equivalent to  $\mathcal{C}$  which differ in only one component ( $\mu_a(C_k)$ ) is  $r(p - 1)$ , where  $r$  is the number of components of  $\mathcal{C}$  which is also the number of factors of  $Y^m - 1$ . Similarly, the number of equivalent quasi-cyclic codes which differ from  $\mathcal{C}$  in only two components ( $\mu_a(C_k)$  and  $\mu_b(C_h)$ ) is equal to  $\binom{r}{2}(p - 1)^2$ . Then the total number of quasi-cyclic codes equivalent to  $\mathcal{C}$  is equal

$$\sum_{k=0}^r \binom{r}{k} (p - 1)^k = p^r.$$

$\square$



## 5 Isodual Quasi-Cyclic Codes

In this section, conditions are given on the existence of isodual quasi-cyclic codes over  $\mathbb{F}_q$ . We start with the following obvious lemma.

**Lemma 5.1** *If there exists an isodual quasi-cyclic code of index  $l$ , then  $l$  must be even.*

**Proof.** From Theorem 3.7, a condition for the existence of an isodual quasi-cyclic code is that the constituent codes  $C_i$ ,  $1 \leq i \leq s$ , are linear isodual codes of length  $l$ . This is possible if and only if  $l$  is even.  $\square$

**Remark 5.2** *From Lemma 5.1 if  $l = p$  odd, then none of the  $p^r$  equivalent codes of the quasi-cyclic code  $\mathcal{C}$  of length  $p \cdot m$  given in Theorem 4.5 can be the dual of the code  $\mathcal{C}$ .*

The results in the remainder of this section are based on the existence of isodual cyclic codes. Thus we first consider the existence of these codes.

Recall that the multiplier given in (9) is a special kind of permutation which characterizes the equivalence of some codes. This multiplier also acts on polynomials of  $R[x]$  and thus gives the following ring automorphism

$$\begin{aligned} \mu_a : R[x]/(x^n - 1) &\longrightarrow R[x]/(x^n - 1) \\ f(x) &\mapsto \mu_a(f(x)) = f(x^a). \end{aligned} \tag{9}$$

If  $C$  is a cyclic code generated by  $f(x)$ , then  $\mu_a(C) = \langle f(x^a) \rangle$ . Thus two cyclic codes  $C = \langle f(x) \rangle$  and  $D = \langle g(x) \rangle$  are multiplier equivalent if there exists a multiplier  $\mu_a$  such that  $g(x) = \mu_a(f(x)) = f(x^a)$ . This justifies our previous statement that the concept of multiplier equivalent quasi-cyclic codes is more general than that given in [9].

**Proposition 5.3** *Let  $C$  be a cyclic code of length  $n$  over  $\mathbb{F}_q$  generated by the polynomial  $g(x)$  and  $\lambda \in \mathbb{F}_q^*$  such that  $\lambda^n = 1$ . Then the following holds*

- (i)  $C$  is equivalent to the cyclic code generated by  $g^*(x)$ , and
- (ii)  $C$  is equivalent to the cyclic code generated by  $g(\lambda x)$ .

**Proof.**

- (i) Consider the multiplier

$$\begin{aligned} \mu_{-1} : \mathbb{F}_q[x]/(x^n - 1) &\longrightarrow \mathbb{F}_q[x]/(x^n - 1) \\ f(x) &\mapsto \mu_{-1}(f(x)) = f(x^{-1}), \end{aligned} \tag{10}$$

which is a ring automorphism. Assume that  $\deg(g(x)) = r$ . If  $C_1$  is the code generated by  $g^*(x)$ , then  $C_1 = \{x^r g^{-1}(0) \mu_{-1}(g(x)) f(x) \pmod{x^n - 1}; f(x) \in \mathbb{F}_q[x]/(x^n -$

1)). Clearly  $\{x^r f(x) \pmod{x^n - 1}; f(x) \in \mathbb{F}_q[x]/(x^n - 1)\} = \{\mu_{-1}(a(x)) \pmod{x^n - 1}; a(x) \in \mathbb{F}_q[x]/(x^n - 1)\}$ , so that  $C_1 = \{g(0)^{-1} \mu_{-1}(g(x)a(x)) \pmod{x^n - 1}; a(x) \in \mathbb{F}_q[x]/(x^n - 1)\} = \mu_{-1}(C)$ . Hence  $C$  is equivalent to  $C_1$  because  $\mu_{-1}$  is a permutation of the coordinates  $\{1, x, x^2, \dots, x^{n-1}\}$ .

(ii) Suppose there exists  $\lambda \in \mathbb{F}_q^*$  such that  $\lambda^n = 1$  and let

$$\begin{aligned} \phi : \mathbb{F}_q[x]/(x^n - 1) &\longrightarrow \mathbb{F}_q[x]/(x^n - 1) \\ f(x) &\longmapsto \phi(f(x)) = f(\lambda x). \end{aligned}$$

Clearly  $\phi$  is a ring automorphism of  $\mathbb{F}_q[x]$ . Since  $\phi(f(x) + h(x)(x^n - 1)) = \phi(f(x)) + \phi(h(x))(x^n - 1)$  as  $(\lambda x)^n - 1 = x^n - 1$ ,  $\phi$  is well-defined on the ring  $\mathbb{F}_q[x]/(x^n - 1)$  and is a ring automorphism of  $\mathbb{F}_q[x]/(x^n - 1)$ . Let  $C_2$  be the cyclic code generated by  $g(\lambda x)$ . Arguing as in part (i),  $C_2 = \phi(C)$ . Then because  $\phi$  is a diagonal matrix on the coordinates  $\{1, x, x^2, \dots, x^{n-1}\}$ , so that  $C$  is equivalent to  $C_2$ .

□

**Proposition 5.4** *Let  $n$  be a positive integer. If  $f(x)$  and  $g(x)$  are polynomials in  $\mathbb{F}_q[x]$  such that*

$$x^n - 1 = g(x)f(x), \tag{11}$$

*then the cyclic code generated by  $g(x)$  is equivalent to the dual of the cyclic code generated by  $f(x)$ .*

**Proof.** Let  $C_1$  the cyclic code generated by  $g(x)$  and  $C_2$  the cyclic code generated by  $f(x)$ . Since the dual of  $C_2$  is generated by  $g^*(x)$ , by Proposition 5.3(i)  $C_1$  is equivalent to  $C_2^\perp$ . □

**Theorem 5.5** *Let  $s$  be an odd integer and  $f(x)$  a polynomial over  $\mathbb{F}_q$  such that  $x^s - 1 = (x - 1)f(x)$ . Then the cyclic codes of length  $2s$  generated by  $(x - 1)f(-x)$  and  $(x + 1)f(x)$  are isodual codes.*

**Proof.** If  $x^s - 1 = (x - 1)f(x)$ , then  $x^s + 1 = (x + 1)f(-x)$  and

$$x^{2s} - 1 = (x^s - 1)(x^s + 1) = (x - 1)f(x)(x + 1)f(-x).$$

Let  $g(x) = (x - 1)f(-x)$  be the generator polynomial of a cyclic code  $C$ . Then the dual code  $C^\perp$  is generated by

$$h^*(x) = (x + 1)f^*(x) = g^*(-x).$$

Hence from Proposition 5.3(i),  $C$  is equivalent to the cyclic code generated by  $g^*(x)$ . Further, from Proposition 5.3(ii), the cyclic code generated by  $g^*(x)$  is equivalent to the cyclic code generated by  $g^*(-x) = h^*(x)$ , as the latter code is  $C^\perp$ , so that  $C$  is isodual. The same result holds for  $g(x) = (x+1)f(x)$ .  $\square$

**Theorem 5.6** *There exists no self-dual or isodual multiplier quasi-cyclic codes with cyclic constituents over  $\mathbb{F}_q$  if  $q$  is odd. When  $l = 2$ , there always exists a quasi-cyclic code with cyclic constituent codes which is isodual. Further there exists an isodual quasi-cyclic code over  $\mathbb{F}_q$  of index  $l = 2s$  for  $s$  odd.*

**Proof.** Assume the existence of a quasi-cyclic code with cyclic constituents which is also self-dual code, respectively isodual. Hence for  $1 \leq s$  the constituent  $C_i$  must be cyclic and self-dual, respectively cyclic isodual code that is from Theorem 3.7 and Proposition 4.2. It is well known that there exists no cyclic self-dual codes cyclic codes [6], respectively there no cyclic multiplier isodual code if  $q$  is odd. If  $l = 2$ , then  $x^2 - 1 = (x-1)(x+1)$ , and so from Proposition 5.3(i) the code generated by  $(x-1)$  is equivalent to the code generated by  $x+1$ , which is its dual. We consider the quasi-cyclic code with cyclic constituent codes  $C_i = \langle (x-1)f(x) \rangle$  and  $C'_j = C_j'' = \langle (x-1)f(x) \rangle$ . Since  $C'_j = C_j''$  and they are over the same field extension (the degree of  $g$  is the same as of  $g^*$ ), the result follow from Theorem 3.7.  $\square$

## References

- [1] L. Babai, P. Codenotti, and J. A. Grochow, *Code equivalence and group isomorphism*, in Proc. ACM-SIAM Symp. on Discr. Algorithms, San Francisco CA, 1395–1408, 2011.
- [2] N. Brand, *Polynomial isomorphisms of combinatorial objects*, Graphs and Combin. 7(1), 7–14, 1991.
- [3] W. C. Huffman, V. Job, and V. Pless, *Multiplier and generalized multipliers of cyclic objects and cyclic codes*, J. Combin. Theory A 62, 183–215, 1993.
- [4] W. C. Huffman, *Codes and groups*, in V. S. Pless and W. C. Huffman, Eds., Handbook of Coding Theory, Elsevier, Amsterdam, 1345–1439, 1998.
- [5] G. Ganske and B. R. McDonald, *Finite local rings*, Rocky Mountain J. Math. 3(4), 521–540, 1973.
- [6] Y. Jia, *On self-dual cyclic codes and generalized self-dual cyclic codes*, Ph.D Thesis, Nanyang Technology University, Singapore, Dec. 2011.

- [7] C. J. Lim, *Quasi-cyclic codes with cyclic constituent codes*, Finite Fields App. 13, 516–534, 2007.
- [8] S. Ling and P. Solé, *On the Algebraic structure of quasi-cyclic codes I*, IEEE Trans. Inform. Theory 30, 113–130, 2003.
- [9] S. Ling and P. Solé, *On the algebraic structure of quasi-cyclic codes III: Generator theory*, IEEE Trans. Inform. Theory 51(7), 2692–2700, 2005.
- [10] R. J. McEliece, *A Public-Key Cryptosystem Based On Algebraic Coding Theory*, DSN Progress Report 42-44, 114–116, Jan.-Feb. 1978.
- [11] A. Otmani, J. P. Tillich, and L. Dallot, *Cryptanalysis of a McEliece cryptosystem based on quasi-cyclic codes*, in Proc. Conf. on Symbolic Computation and Crypt., Beijing, China, 69–81, Apr. 2008.
- [12] N. Sendrier, *Finding the permutation between equivalent linear codes: The support splitting algorithm*, IEEE Trans. Inform. Theory 26, 1193–1203, 2000.
- [13] N. Sendrier and D. E. Simos, *The hardness of code equivalence over  $\mathbb{F}_q$  and its application to code-based cryptography*, in P. Gaborit (Ed.) Post-Quantum Cryptography - PQCrypto 2013, LNCS 7932, Limoges, France, Springer, 203–216, 2013.